# Exhibit A

JAN 0 8 2003

BLAKELY, SOKOLOFT TAYLOF & LAFMAN LLP
COSTA MESA

# RECEIVED

JAN 0. 8 2004

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

Docket #: 42390.P9844 Application No.: 09/571,899 Filing Date: 12/27/2000 Date Mailed: 12/12/2003 Due Date(s): Atty/Sec: WWS/JAH/crr Client: INTEL CORPORATION Title: A Platform and Method for Creating a Secure Boot that Enforces Proper User Authentication and Enforces Hardware Configurations First Named Inventor: David W. Grawrock The following has been received in the U.S.P.T.O. on the date stamped hereon: Certificate of Mailing Fee Transmittal (original & copy) Information Disclosure Statement & PTO/SB/08 (4 pgs) Transmittal Letter Cited References Check No. 14668 in the amount of \$180.00 Postcard

SECFINED

Assignee: Intel Corporation

JAN - 7 2004

"AREL". OUNOLOFF, TAYLOH & ZAFMAN SUNNYVALE

usbank CAL HUNDRED EIGHTY AND NOX LOOK Director of the United States Patent and Fredemark Office

ATE

DESCRIPTION

2/8/2003

U.S. Patent and Trademark Office IDS fee for A Platform and Method of Creating a Secure Boot that Enforces Proper User Authentication and Enforces Hardware Configurations MOD BIBALIANA TOBE

App. No.; .. 09/751,899 Filewd: 12/28/00 042390.P9844 WW5/crr intel Corporation

AMOUNT

\$ 180.00

14668

લેલા જ્વારા કારણ જો <mark>તે જે સામાના સુર્વે કે મુક્સ માર્</mark>કા કરો છે. જે કે સ્ટેક્સ્ટ્રેન્ટ કે સ્ટ્રેન્ટ કે સ્ટ્રેન્ટ કે સ્ટ્રેન્ટ ફેસ્ટ્રેન્ટ કે સ્ટ્રેન્ટ ફેસ્ટ્રેન્ટ ફેસ્ટ્ટ ફેસ્ટ્રેન્ટ ફેસ્ટ્રેન્ટ ફેસ્ટ્રેન્ટ ફેસ્ટ્રેન્ટ ફેસ્ટ્રેન્ટ ફેસ્ટ્રેન્સ્ટ્રેન્સ્ટ્રેન્ટ ફેસ્ટ્રેન્સ્ટ્રેન્સ્ટ્રેન્સ્ટ ફેસ્ટ્રેન

TRANSMITTAL FORM		Application No.	09/571,899		
		Filing Date	December 27, 2000		
(to be used for all correspondence afte	r ınıtıaı tılıng)	First Named Inventor	David W. Grawrock		
•		Art Unil	2131		
		Examiner Name	Unassigned		
Total Number of Pages in This Submissi	on	Attorney Docket Number	42390P9844		
ENCLO	SURES (chec	k all that apply)			
Fee Transmillal Form	Drawing(s)		After Allowance Communication to Group		
Fee Allached	Licensing-7	related Papers	Appeal Communication to Board of Appeals and Interferences		
Amendment / Response	Petition		Appeal Communication to Group (Appeal Nodea, Brief, Raply Brief)		
After Final Aftidavits/declaration(s)	Pelition to Provisional	Convert a Application	Proprietary Information		
Extension of Time Request	Power of A Change of	ltorney, Revocation Correspondence Address	Status Letter		
Express Abandonment Request	Terminal Disclaimer		Other Enclosure(s) (please identify below):		
Information Disclosure Statement	Request fo	r Refund	Cited References		
≥ PTO/SB/08	CD, Numbe	er of CD(s)			
Certified Copy of Priority Document(s)					
Rosponse to Missing Parts/ Incomplete Application	Remarks		<u> </u>		
Basic Filing Fee					
Declaration/POA  Response to Missing					
Response to Missing Parts under 37 CFR 1.52 or 1.53					
SIGNATUR	E OF APPLICA	NT, ATTORNEY, OR AC	SENT		
Firm James Henry, R	teg. No. 41,06	4			
ا مسمد المشاهدات	OKOLOFF,	TAYLOR & ZAFM	AN LLP		
Signature					
Date December 12,	2003		· · · · · · · · · · · · · · · · · · ·		
CERTIF	ICATE OF MAIL	ING/TRANSMISSION			
I hereby certify that this correspondence is being deposited with the United States Postal Service on the date shown below with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.					
Typed or printed name   Corrinn R. I	Reyfloids /				
Signature	An Plus	with I	Date December 12, 2003		
Based on PTO/SB/21 (08-03) as modified by Blakely, Solokof SEND TO: Commissioner for Patenta, P.O. Box 1450, Alaxa	r, Taylor & Zalmun (vfs) ndra, VA 22313-1450	09/11/2003.			

FEE TRANSMITTAL			L	Complete if Known										
for FY 2003			<u> </u>				/571,899							
•			-		-							December 27, 2000		
EI	ilective	01/01/200	23. Pai	tont feus aro subja	ct io annual	revision.	Ê	First Named Inventor			Dav	id W. Graw	Tock	
App	licant	claims	smal	l entity status.	. See 37	CFR 1.27.	E	Examiner Name			Una	ssigned		
<u> </u>	_			<del>-</del>				Group/Art	Unit		213			
1012	T AM	IOUNT	OF P	AYMENT	(\$)	180	.00	Allorney	ocke	ι No.	4239	0P9844	,	
METHOD OF PAYMENT (check all that apply)				apply)				FE	E CALCULATI	ON (continue	∍d)			
Chack Credit card Money Other None				П.,	3. A	OITIDO	NAL	FEES						
	_		•	Order	Other	☐ None	1	e Entity	Sma	li Entity				
Caposil A	ACCOUNT	ı					Fee	Foo	Fee	Fee	-			
Deposit	$\overline{}$						Code		Code	( <del>s</del> )	Fe	e Description		Fee Paid
Account Number	L.			02-2666			1051	190	2051	65	Surcharge - late fibrig	fee or outh		
Orspesit	$\equiv$						1052	50	2002	25	Surcharge - tale prov			
Account Name	BI	akely,	Soko	oloff, Taylor	& Zafn	nan LLP	l				cover sheet			
	——						2053	130	2053 1812	130 2,520	Non-English specific			
i				t ( check all that a	•		1812	-	ľ	-	For Ming a request fo Requesting publication		300A	
Charge to	96(8) i/	dicated be	510~v	□ c∞	qg suà oncu	ayments	1804	920 *	1804	920	Examiner action	an or silk phorio		
=				ired under 37 CFF xcapt for the filing		17. 1 18 and 1.20.	1805	1.840	1805	1,840 1	Requesting publication	on of SIR efter		
	ove-ide	ntiled de	008 # 30	CONTR.	9		1251	110	2251	55	Extension for reply w	whin first month		<del></del>
		FEI	E CA	LCULATION	N		1252	420	2252	210	Extension for reply w	ithin second month		<u> </u>
1. BA	Sic	FILING			•		1253	950	2253	475	Exignation for reply w	thin third month		<del>  </del>
Large Entity		Small E		-			1254		2254	740	Extension for reply w	thin fourth month		<u> </u>
For F	œ.	Foe	Fee	Fee Description		Fee Paid	1255		2255	505	Extension for reply w			<b> </b>
Codo (	F9 (	Code	<del>(2)</del>			7337.				165	Notice of Appeal			
1001	770	2001	362	Utility (liling fee			1404		2401	185	• •	a of an agency		<u> </u>
1002	340	2002	170	Design filing fee	,		1402		2402		Fing a brief in suppl			
1003	530	2003	265	Plant filing fee			1403		2403	145	Request for oral hea	-		
	770	2004	385	Raissue filing fa	0		1451		2451	1,510	Petition to institute a		ing	
1005	180	2005	80	Provisional filing	leo		1452		2452	55	Petition to revive - ur			
			\$UBT	OTAL (1)	(3)		1453		2453	665	Petition to revive - ur			
					<del></del>		1501		<b>7501</b>	665	Littlify is sue fee (or re	ensus)		
2. EX	IKA	CLAII	M FE	ES them	Pee from	Fee Pald	1502		2502	240	Design issue fee			<u> </u>
Total Claima	Г			CENTRE 1	bolow	1-	1503		2503	320	Plant lasue fee			
tridependent	ŀ	<b>—</b> 1:		┇┝╼╌┤╩╏		<u> </u>	1460		2460	130	Pelilions to the Com			
Claims			3	`LX		<u>                                     </u>	1807		1807		Processing fee under			L
Multiple Dapar	-cent			i		J` <u>L</u>	180G		1806	180	Submission of Inform		lu)	180.00
Foo Fo			Foe	Fee Description			8021	40	8021	40	Recording each paid property (times number			
ŀ	18	2202	ρ) (A)	Caims in excess	of 20		1809	770	1809	385	Filing a submission a (37 CFR § 1.129(2))	fter final rejection		
1201 - 0	90	2201	43	Independent claim	ns in excess	of 3	1810	770	2810	985	For each additional in			
1203 29	<b>20</b>	2203	145	Multiple Depende	nt dalm. If n	ól páid			١		examined (37 CFR §	****		
1204 6	96	2204	43	**Réissuo Indeper palent	ndent eleima	ovet outdins;	1801		1802	385 900	Request for Continue Request for expedite	d examination	E)	
1205 1	18	2205	9	"Reissue cleims l original palem	n excess of	20 and over	Other f	os (spectly)	,		of a design application	n 		
			SUBI	OTAL (2)	(\$)									
••,	יייוטס זכ	oer previou		ld, if greater, For R		n below	"Reduce	d by Basic Film	g Fee Pa	d		SUBTOTAL (3)	(\$)	180.00
			-, -,	B-ANA-1 (A) 1)			<u> </u>					<del></del>		
SUBMI	ITTE	D BY					- 1 -		- 62			Comp	lete (if applic	
Name (P	rin vTyp	ж) <b>ј</b> ј:	ames	Henry		,		Registretic Atlamey/Age		] 4	11,064	Telaphone	(714) 55	7-3800
<u> </u>			-	<del>-///</del>					*	1	,	-		
Şignatu			1_	C#1								Date	12/1	2/03
Based on PTO/ SEND TO: Cor	SB/17	(08-03) at	model stents.	er by Blately, Sol	Skoff, Taylor Jexandria, V	& Zalman (wr) (18/1 A 22913-1450	1/2003.					-		

FEE TRANSMITTAL		Complete if Known						
for FY 2003		<del></del>	Application Number 09/571,899					
		Filing Date				ecember 27, 2		
Effective 01/01/2003. Patent fees are subject to annual mulsion,		First Name				avid W. Graw	TOCK	
Applicant claims small entity status. See 37 CFR 1.27.		Examiner		<del>}</del>		nassigned		
TOTAL AMOUNT OF PAYMENT (\$) 180.	00	Group/Art				31	<del></del> .	
(0) 180.		Allomey C	ocke	140.	1 42	390P9844		
METHOD OF PAYMENT (check all that apply)		,		FE	E CALCULA	TION (continue	ed)	
S Check ☐ Credit card ☐ Money ☐ Other ☐ Nune	3.	ADDITIO	NAL	FEE\$	;			
Depose Account	La	arge Entity	Sma	li Entity				
	Fo		Fag	Foe	<del>-</del>			
Account 02-2666	Co		Code	(E)		Fee Description		Fee Paid
Number	103		2051 2052	65 25	Surcherge - tale f	lling fee or oath provisional lifing fee or		
Account Account Blakely, Sokoloff, Taylor & Zafman LLP	"	- ~	2000		cover sheet.	· ·		1 []
Name Diakery, Sokoloff, Taylof & Zafffall LLF	20	53 130	2053	130	Non-English sper	alication		
The Commissioner is authorized to: ( check all that apply)	18	1	1812	2,520		i lor ex perte reexam <sub>i</sub> n	alion	
Charge lee(s) indicated below Credit any overpayments	1 H	04 920	1904	920 •	Requesting public Examiner action	alion of SIR prior to		
Charge any additional feets) required under S7 CFR §§ 1.18. 1.17, 1.18 and 1.20.	10	05 1,8-10 *	1805	1.840	Requesting public Examiner action	cation of SIR after		
Charge (se(s) indicated below, except for the filling fee to the above-identified deposit account	12:	51 170	2251	55	Extension for repl	y within first month		
FEE CALCULATION	72		2252	210		, y within second month		
1. BASIC FILING FEE	12		2253	475	Extension for repl	y within third month		<u> </u>
Large Entity Small Entity	12		2254	740	Extension for repl	y within fourth morath		
Foo Foo Foo Foo Foo Description Fee Paid		55 1,210	2255	605	Extension for repl	y within 16th month		
Codo (S) Codo (S)	14		2401	165	Notice of Appual			
1001 770 2001 305 Utility fling fee	14	02 330	2402	165	Filing a brief in su	Ipport of an apposal		
1002 340 2002 170 Design filting fee	14	ტე 290	2403	145	Request for oral i	nearing		
1003 530 2003 266 Plant filing (se 1004 770 2004 366 Retssue filing (se	14	51 1,510	2451	1,510	Petition to institu	o a public use proceed	ng	,
1005 100 2005 80 Provisional filing fee	14	110 E2	2452	55	Petition to revive	- unavoidable		<b></b>
	14	53 1,330	2453	665	Petition to revive	- unintentional		_ <del>[                               </del>
SUBTOTAL (1) (\$)	15	iot 1,330	2501	685	Utility issue fee (d	y reissue)		
2. EXTRA CLAIM FEES Bota Fee from	15	iO2 480	2502	240	Dealgn issue fee			
Total Claims Fee Paid	. 15	640	2503	320	Plant issue fee			
1 1 1 20 a1  X1   T	14	60 130	2460	130	Politions to the C	ommissioner		~~~
Independent 3 = X	18	107 50	1807	50	Processing fee un	der 37 CFR 1,17(q)		
Multiple Dependent	18	06 180	1806	180	Submission of In	formation Disclosure St	mt.	180.00
Large Entity Small Entity Fee Fee Fee Fee Fee Fee Description	90	121 40	8021	40		palant assignment per umber of properties)		
Code (5) Code (5) 1202 18 2202 9 Claims in excess of 20	18	170	1809	395	Filing a submissio (37 CFR § 1.129)	n after finat rejection 8))		
1201 86 2201 43 Independent claims in gross of 3 1203 290 2203 145 Multiple Dependent claim, if not paid	18	110 770	2810	385	For each addition examined (37 CF			
1204 88 2204 43 "Reissue independent claims over original	18	101 770	2901	385	Request for Conti	inued Examination (RC	E)	<b> </b>
polent	18	102 900	1802	900	Request for expe			
1205 18 2205 9 "Reissue dislate in excess of 20 and over original patent	Othe	or fee (specily)	1		of a design applic	- Nove		
	ŧ			-			<del></del>	
SUBTOTAL (2) (8) "or number previously paid, if greater, For Relasties, see below	*Red	Load by Basic Film	g Fee Pa	ki		SUBTOTAL (3)	(\$)	180.00
SUBMITTED BY						Comp	lete (if applic	able)
Name (Print/Type) James Henry		Registratio (Attorney/Age		- 4	11,064	Telephone	(714) 55	
Signature		y storieties de				Date		2/03
Basad on PTO/SB/17 (09-03) as modified by Flightsky, Schokerf, Taytor & Zarman (wtr) 08/11 SEND TO: Commissioner for fratoms, P.O. Box 1450, Alexandria, VA 22315-1450	1/2003	<del>.</del>	-			12010		ــــــــــــــــــــــــــــــــــــــ
SEND TO: Commissioner for Patonts, P.O. (90x 1450, Alexandria, VA 22315-1450								

Docket No.: 42390P9844

#### IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re the Application of:

DAVID W. GRAWROCK

Application No.: 09/571,899

Filed: December 27, 2000

For: A Platform and Method for Creating a

Secure Boot that Enforces Proper User Authentication and Enforces Hardware

Configurations

Art Group: 2131

Examiner: Unassigned

#### INFORMATION DISCLOSURE STATEMENT UNDER 37 C.F.R. §1.97

Commissioner for Patents P.O. Box 1450 Alexandria, VA 22313-1450

Sir:

In accordance with the duty of disclosure, enclosed is a copy of Information Disclosure Statement by Applicant (form PTO/SB/08), which is being submitted before the mailing of a final Office Action. It is respectfully requested that the cited references be considered and that the enclosed copy of PTO/SB/08 be initialed by the Examiner to indicate such consideration and a copy thereof returned to applicant(s). Copies of the references cited on PTO/SB/08 are enclosed herewith.

The submission of this Information Disclosure Statement is not to be construed as a representation that a search has been made in the subject application and is not to be construed as an admission that the information cited in this statement is material to patentability.

Applicant has concurrently submitted an electronic Information Disclosure Statement (IDS) for the above-referenced patent application. In the concurrently filed electronic IDS submission, it was requested that any requisite fees be debited from Deposit Account 02-2666. Applicant respectfully requests that only one fee be debited for these concurrently filed IDS submissions if such fees are required.

Respectfully, submitted,

BLAKELY, SAKOLOFE, PAYLOR & ZAFMAN LLP

James Henry, Rog. No. 41,064

12400 Wilshire Boulevard, 7th Floor Los Angeles, CA 90025

Telephone: (714) 557-3800

Date: December 12, 2003

I hereby certify that this correspondence is being deposited with the United States Postal Service on the date shown below with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Ruguolds

Corrinn R. Reynolds

Date

12-12-03

PROPERTY OF CONTRACT A STATE OF CONTRACT OF CO Substitute for form 141BA/PTO Complete if Known INFORMATION DISCLOSURE **Application Number** 09/571,899 STATEMENT BY APPLICANT Filing Date December 27, 2000 First Named Inventor David W. Grawrock **Group Art Unit** 2131 **Examiner Name** Unknown Attorney Docket No: 042390.P9844 Sheel 1 of 2

		FOREIGN PA	TENT DOCUMENTS			
Examiner Initials*	Foreign Document No	Publication Date	Name of Patentee or Applicant of cited Document	Class	Subclass	. 12
	DE-DE4217444	12/03/1992	Toyohisa, Imada, et al.	}		abs
	EP-EP0473913	03/11/1992	Farrell, Joel A.			
	EP-EP0600112	06/08/1994	Wimmer, Manfred D.			abs
	EP-EP0930567	07/21/1999	Brewer, Jason M.			
	EP-EP1030237	08/23/2000	Proudler, John, et al.	1		
	EP-EP1146715	10/17/2001	Wang, Xin, et al.			
	JP-JP2000076139	03/14/2000	Tanno, Masaaki , et al.			~
	WO-WO0062232	10/19/2000	Headrick, Samual P., et al.			
	WO-WO0127723	04/19/2001	Vamvakas, Athanasia, et al.			
	WO-WO0127821	04/19/2001	Chen, Liqun, et al.			
	WO-WO0175564	10/11/2002	Herbert, Howard C., et al.			
	WO-WO0175565	10/11/2001	Ellison, Carl M.			
	WO-WO0175595	10/11/2001	Ellison, Carl M., et al.			l
	WO-WO02086684	10/31/2002	Proudler, Graeme J.			
	WO-WO0217555	02/28/2002	Ford, Warwick			
	WO-WO9729567	08/14/1997	Gressel, Carmi, et al.			
	WO-WO9834365	08/06/1998	Devanbu, Premkumar T., et al.			
	WO-WO9844402	10/08/1998	Bramhilf, Ian D., et al.			
	WO-WO9905600	02/04/1999	Garst, Blaine, et al.			
	WO-WO9909482	01/15/2002	Bausch, Jean			
	WO-WO9957863	11/11/1999	Hayes Jr., Kent F., et al.			

	ÖTHE	R DOCUMENTS NON PATENT LITERATURE DOCUMENTS	
Examiner Initials*	Çite No *	Include name of the author (in CAPITAL LETTERS), this of the article (when appropriate), this of the from (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T²
		BERG, CLIFF, "How Do I Create a Signed Applet?", Dr. Dobb's Journal, (08/1997),1-9	
		BRANDS, STEFAN, "Restrictive Blinding of Secret-Key Certificates", SPRINGER-VERLAG XP002201306, (1995), Chapter 3	
		CHEN, ANDREW A., et al., "Safe and Protected Execution for the Morph/AMRM Reconfigurable Processor", 7th Annual IEEE Symposium, FCCM '99  Proceedings, XP010369180, ISBN 0-7695-0375-6, Los Alamitos, CA, (4/21/1999),209-221	
		COMPAQ COMPUTER CORPORATION, et al., "Trusted Computing Platform Alliance (TCPA) Main Specification Version 1.1a", (12/2001),1-321	
		DAVIDA, GEORGE I., et al., "Defending Systems Against Viruses through Cryptographic Authentication", Proceedings of the Symposium on Security and Privacy, IEEE Comp. Soc. Press, ISBN 0-8186-1939-2, (May 1989),	
		GOLDBERG, ROBERT P., "Survey of Virtual Machine Research", <u>COMPUTER</u> Magazine, (06/1974), cover, contents, 34-35	

EXAMINER	DATE CONSIDERED

SUSCIMED POSSIVE PROPERTY PORT (#10-1442)

\*EXAMINER\* Initial If reference considered, whether or not citation is in contempance that first form with ment communication at check mark here if English language Translation is attached to provide statement that is place a check mark here if English language Translation is attached.

PTORBUCKATIOUS Approval for use disough 10/31/2009 OAKI 651-0001 rd 8 Treferige Office, U.S. DEPARTMENT OF COMMETICE

Substitute for form 1448A/PTO INFORMATION DISCLOSURE	Complete il Known					
STATEMENT BY APPLICANT	Application Number	09/571,899				
(Use us many sheels as necessary)	Filing Date	December 27, 2000				
	First Named Inventor	David W. Grawrock				
	Group Art Unit	2131				
	Examiner Name	Unknown				
Sheel 2 of 2	Attorney Docket No: 0	042390.P9844				

	GONG, LI, et al., "Going Behond the Sandbox: An Overview of the New Security	
	Architecture in the Java Development Kit 1.2", Proceedings of the USENIX	
	Symposium on Internet Technologies and Systems, Monterey, CA,(12/1997),	
]	GUM, P. H., "System/370 Extended Architecture: Facilities for Virtual	
1	Machines", IBM J. Research Development, Vol 27, Number 6, (11/1983),530-	
1	544	
	HEINRICH, JOE, "MIPS R4000 Microprocessor User's Manual, Second	
1	Edition", Chapter 4 "Memory Management", (6/11/1993),61-97	
	IBM, "Information Display Technique for a Terminiate Stay Resident Program	
	IBM Technical Disclosure Bulletin", TDB-ACC-No. NA9112156, Vol. 34, Issue	
	7A, (12/1/1991),156-158	
	INTEL, "Intel386 DX Microprocessor 32-Bit CHMOS Microprocessor With	_
	Integrated Memory Management", (1995), 1-56	
	KARGER, PAUL A., et al., "A VMM Security Kernal for the VAX Architecture",	
	Proceedings of the Symposium on Research in Security and Privacy,	
1	XP010020182, ISBN 0-8186-2060-9, Baxborough, MA, (5/7/1990),2-19	
<u> </u>	KASHIWAGI, KAZUHIKO , et al., "Design and Implementation of Dynamically	_
	Reconstructing System Software", Software Engineering Conference,	
1.	Proceedings 1996 Asia-Pacific Seoul, South Korea 4-7 Dec. 1996, Los Alamilos,	
	CA USA, IEEE Comput. Soc. US, ISBN 0-8186-7638-8,(1996),	
ļ	LAWTON, KEVIN, et al., "Running Multiple Operating Systems Concurrently on	
1	an IA32 PC Using Virtualization Techniques".	
	http://www.plex86.org/research/paper.txt, (11/29/1999),1-31	
<del></del>	LUKE, JAHN , et al., "Replacement Strategy for Aging Avionics Computers",	—
	IEEE AES Systems Magazine, XP002190614,(March 1999),	
<del></del>		
	MENEZES, OORSCHOT, "Handbook of Applied Cryptography", CRC Press	
<del> </del>	LLC, USA XP002201307, (1997),475	
<b></b>	MOTOROLA, "M68040 User's Manual", (1993), cover, vi-xxiii, 1-1 to 8-32	
1	RICHT, STEFAN, et al., "In-Circuit-Emulator Wird Echtzeittauglich", Elektronic,	
	Franzis Verlag GMBH, Munchen, DE, Vol. 40, No. 16, XP000259620,(100-	
	103),8-6-1991	
i i	ROBIN, JOHN S., et al., "Analysis of the Pentium's Ability to Support a Secure	
1	Virtual Machine Monitor", Proceedings of the 9th USENIX Security Symposium,	
	XP002247347, Denver, Colorado, (8/14/00),1-17	
1	ROSENBLUM, M., "Virtual Platform: A Virtual Machine Monitor for Commodity	
	PC", Proceedings of the 11th Hotchips Conference, (8/17/1999),185-196	_
	SAEZ, SERGIO, et al., "A Hardware Scheduler for Complex Real-Time	
	Systems", Proceedings of the IEEE International Symposium on Industrial	
	Electronics, XP002190615,(July 1999),43-48	
1	SHERWOOD, TIMOTHY, et al., "Patchable Instruction ROM Architecture",	_
1	Department of Computer Science and Engineering, University of California, San	
	Diego, La Jolla, CA, (Nov. 2001), 24-33	

EXAMINER	DATE CONSIDERED

# UNITED STATES PATENT AND TRADEMARK OFFICE **ACKNOWLEDGEMENT RECEIPT**

Electronic Version 1.1 Stylesheet Version v1.1.1

Title of Invention

A Platform and Method of Creating a Secure Boot That Enforces Proper User Authentication and Enforces Hardware Configurations

Submission Type:

Information Disclosure Statement

Application Number:

09/751899

\*09/751899\*

EFS ID:

52214

Server Response:

Confirmation Code	Message
ISVR1	Submission was successfully submitted - Even if Informational or Warning Messages appear below, please do not resubmit this application
ICON1	9094
ISYS5	Filename≖ N/A BusinessRule= Validation System/Function Call Information. #Supporting Msg:Server unable to validate the Confirmaton/Application numbers at this time. They will be checked by PTO personnel later.

First Named Applicant:

**Grawrock David** 

Attorney Docket Number: 42P09844

Timestamp:

2003-12-12 20:31:43 EDT

From:

File Listing:

Doc. Name	File Name	Size (Bytes)
us-fee-sheet	42P09844-usfees.xml	1759
us-fee-sheet	us-fee-sheet.xsl	24912
us-fee-sheet	us-fee-sheet.dtd	11069
us-ids	42P09844-usidst.xml	25929
us-ids	us-ids.dtd	7763
us-ids	lex.ebi-eu	12026
package-data	42P09844-pkda.xml	2385
package-data	package-data.dtd	27025
package-data	us-package-data.xsl	19263
	Total files size	132131

Message Digest:

eac3daebdfa3f64dacf2d0e35e7c992c43484def

Digital Certificate Holder

Name:

cn=William W. Schaal,ou=Registered

Attorneys, ou=Patent and Trademark

Office,ou=Department of Commerce,o=U.S. Government,c=US

## FEE TRANSMITTAL

Electronic Version v08 Stylesheet Version v08.0

Title of Invention

A Platform and Method of Creating a Secure Boot That Enforces Proper User Authentication and Enforces Hardware Configurations

Application Number:

09/751899

\*09/751899\*

Date:

2000-12-27

First Named Applicant:

Grawrock David

Attorney Docket Number: 42P09844 Art Unit:

Unknown

Examiner:

Unknown Unknown

# **TOTAL FEE AUTHORIZED \$180**

Patent fees are subject to annual revisions on or about October 1st of each year.

#### BASIC FILING FEE

Fee Description	Fee Code	Amount \$	Fee Paid \$
Submission Of Information Disclosure Stmt Fee	1806	180	180

#### **AUTHORIZED BILLING INFORMATION**

The commissioner is hereby authorized to charge indicated fees and credit any overpayments to:

Deposit account number: 022666

Access Code

Deposit name:

Blakely Sokoloff Taylor Zafman LLP

Deposit authorized name: William W. Schaal

Signature:

William W. Schaal

Date (YYYYMMDD):

2003-12-12

Charge Any Additional Fee Required Under 37 C.F.R. Sections 1.16 and 1.17.

### ELECTRONIC INFORMATION DISCLOSURE STATEMENT

Electronic Version v18 Stylesheet Version v18.0

Title of Invention

A Platform and Method of Creating a Secure Boot That Enforces Proper User Authentication and Enforces Hardware Configurations

Application Number:

09/751899

\*09/751899\*

Confirmation Number:

9094

First Named Applicant:

Grawrock David

Attorney Docket Number: 42P09844

Art Unit:

Unknown

Examiner:

**Unknown Unknown** 

Search string:

( 20010021969 or 20010027527 or 20010037450 or 4037214 or

4247905 or 4278837 or 4319323 or 4347565 or 4366537 or 4521852 or 4571672 or 4759064 or 4795893 or 4825052 or 4907270 or 4907272 or 4910774 or 5022077 or 5075842 or 5079737 or 5139760 or 5255379 or 5293381 or 5293424 or 5317705 or 5386552 or 5421006 or 5434999 or 5437033 or 5442645 or 5455909 or 5459867 or 5459869 or 5473692 or 5479509 or 5504922 or 5511217 or 5522075 or 5528231 or 5533126 or 5566323 or 5568552 or 5590287 or 5606617 or 5615263 or 5628022 or 5630106 or 5657445 or 5717903 or 5720609 or 5721222 or 5729760 or 5737604 or 5737760 or 5757919 or 5764950 or 5764969 or 5796835 or 5796845 or 5805712 or 5825875 or 5835594 or 5844986 or 5852717 or 5854913 or 5867577 or 5872994 or 5890189 or 5900606 or 5901225 or 5901294 or 5903752 or 5937063 or 5953502 or 5970147 or 5978481 or 5987557 or 6014745 or 6055637 or 6058478 or 6075938 or 6085296 or 6092095 or 6101584 or 6115816 or 6125430 or 6148379 or 6158546 or 6175925 or 6178509 or 6182089 or 6192455 or 6205550 or 6222923 or 6249872 or 6252650 or 6269392 or 6272533 or 6272637 or 6282651 or 6282657 or 6292874 or 6301646 or 6308270 or 6314409 or 6321314 or 6339815 or 6339816 or 6357004 or 6374286 or 6374317 or 6378072 or 6389537 or 6397242 or 8412035 or 6421702 or 6435416 or 6445797 or 6463535 or 6499123 or 6505279 or 6507904 or 6535988 or 6557104 or

# **US Patent Documents**

Note: Applicant is not required to submit a paper copy of cited US Patent Documents

6633963 or 6633981 ).pn.

init	Cite.No.	Patent No.	Date	Patentee	Kind	Class	Subclass
	1	20010021969	2001-09-13	Burger, Stephen G., et al.			
	2	20010027527	2001-10-04	Khidekel, Yuri, et al.			
	3	20010037450	2001-11-01	Metlitski, Evgueny A., et al.			
					7		

1			,		
	4	4037214	1997-07-09	Birney, Richard E., et al.	
	5	4247905	1981-01-27	Yoshida, Yukihiro , et al.	711 166
	6	4278837	1981-07-14	Best, Robert M.	
	7	4319323	1982-03-09	Ermolovich, Thomas R., et al.	
	8	4347565	1982-08-31	Kaneda, Saburo , et al.	
	9	4366537	1982-12-28	Karl, M. G.	]
	10	4521852	1985-06-04	Guttag, Karl M.	<u> </u>
	11	4571672	1986-02-18	Hatada, Minoru , et al.	j
	12	4759064	1988-07-19	Chaum,	j
	13	4795893	1989-01-03	Ugon, Michael	]
	14	4825052	1989-04-25	Chemin, Francois , et al.	]
	15	4907270	1990-03-06	Hazard, Michel	<u>.                                    </u>
	16	4907272	1990-03-06	Hazard, Michel	<u> </u>
	17	4910774	1990-03-20	Barakat, Simon	<u> </u>
	18	5022077	1991-06-04	Bealkowski, Richard , et al.	j
	19	5075842	1991-12-24	Lai, Konrad K.	j
	20	5079737	1992-01-07	Hackbarth, Holden G.	711 164
	21	5139760	1994-06-07	Mason, Andrew H., et al.	<u> </u>
	22	5255379	1994-03-08	Melo, Michael D.	
	23	5293381	1994-03-08	Choy, Henry S.	]
	24	5293424	1994-03-08	Hotley, Thomas O., et al.	
	25	5317705	1994-05-31	Gannon, Patrick M., et al.	
	26	5386552	1995-01-31	Garney, John L.	]
	27	5421006	1995-05-30	Jablon, David P., et al.	]
	28	5434999	1995-07-18	Goire, Christian , et al.	] . [
	29	5437033	1995-07-25	Inoue, Taro , et al	·
	30	5442645	1995-08-15	Ugon, Michel , et al.	j
	31	5455909	1995-10-03	Blomgren, James S., et al.	
	32	5459867	1995-10-17	Adams, Phillip M., et al.	
	33	5459869	1995-10-17	Spilo, Michael L.	
	34	5473692	1995-12-05	Davis, Derek L.	
	35	5479509	1995-12-26	Ugon, Michael	]
	36	5504922	1996-04-02	Seki, Yukihiro , et al.	]
	37	5511217	1996-04-23	Nakajima, Atsushi , et al.	
	38	5522075	1996-05-28	Robinson, Paul T., et al.	j
	39	6528231	1996-06-18	Patarin, Jacques	]
	40	5533126	1996-07-02	Hazard, Michel , et al.	]
	41	5566323	1996-10-15	Ugon, Michel	
					1

	42	5568552	1996-10-22	Davis, Derek L.
	43	5590287	1996-12-31	Zeller, Charles P., et al.
	44	5606617	1997-02-25	Brands, Stefanus A.
	45	5615263	1997-03-25	Takahashi, Richard J.
	46	5628022	1997-05-06	Ueno, Masahiro , et al.
	47	5630106	1997-05-13	Ishibashi, Shohzoh
	48	5657445	1997-08-12	Pearce, John J.
	49	5717903	1998-02-10	Bonola, Thomas J.
	50	5720609	1998-02-24	Pfefferle, William C.
	51	5721222	1998-02-24	Bernstein, Peter R., et al.
	52	5729760	1998-03-17	Poisner, David I.
$\overline{\Box}$	53	5737604	1998-04-07	Miller, David A., et al.
	54	5737760	1998-08-07	Grimmer, Jr., George G., et al.
	55	5757919	1998-05-26	Herbert, Howard C., et al.
	56	5764950	1998-06-09	Ishizaki, Norihiko
	57	5764969	1998-06-09	Kahle, James A.
	-58	5796835	1998-08-18	Saada, Charles
	59	5796845	1998-08-18	Serikawa, Mitsuhiko , et al.
	60	5805712	1998-09-08	Davis, Derek L.
	61	5825875	1998-10-20	Ugon, Michel
	62	5835594	1998-11-10	Albrecht, Mark , et al.
	63	5844986	1998-12-01	Davis, Derek L.
	64	5852717	1998-12-22	Bhide, Chandrashekhar W., et al.
	65	5854913	1998-12-29	Goetz, John W., et al.
	66	5867577	1999-02-02	Patarin, Jacques
	67	5872994	1999-02-16	Akiyama, Shin-Ichiro , et al
	68	5890189	1999-03-30	Nozue, Hiroshi , et al.
	69	5900606	1999-05-04	Rigal, Vincent
	70	5901225	1999-05-04	lreton, Mark A., et al.
	71	5901294	1999-05-04	Tran, Cang N., et al.
	72	5903752	1999-05-11	Dingwall, Thomas J., et al.
	73	5937063	1999-08-10	Davis, Derek L.
	74	5953502	1999-09-14	Helbig, Sr., Walter A.
	75	5970147	1999-10-19	Davis, Derek L., et al.
	76	5978481	1999-11-02	Ganesan, Ramanaл V., et al.
	77	5987557	1999-11-16	Ebrahim, Zahir
	78	6014745	2000-01-11	Ashe, Vincent
	79	6055637	2000-04-25	Hudson, Jerome D., et al.

711 163

	80	6058478	2000-05-02	Davis, Derek L.	·
	81	6075938	2000-06-13	Bugnion, Edouard , et al.	]
	82	6085296	2000-07-04	Karkhanis, Nitin Y., et al.	
	83	6092095	2000-07-18	Maytal, Benjamin	
	84	6101584	2000-08-08	Satou, Mitsugu , et al.	]
	85	6115816	2000-09-05	Davis, Derek L.	
	86	6125430	2000-09-26	Noel, Karen L., et al.	
	87	6148379	2000-11-14	Schimmel, Curt F.	
	88	6158546	2000-12-12	Hanson, Roger D., et al.	
	89	6175925	2001-01-16	Nardone, Joseph M., et al.	]
	90	6178509	2001-01-23	Nardone, Joseph M.	
	91	6182089	2001-01-30	Ganapathy, Narayanan , et al.	
	92	6192455	2001-02-20	Bogin. Zohar , et al.	]
	93	6205550	2001-03-20	Nardone, Joseph M., et al.	]
	94	6222923	2001-04-24	Schwenk, Joerg	
	95	6249872	2001-06-19	Wildgrube, Frank L., et al.	713 200
	96	6252650	2001-06-26	Nakaumra, Kouji	]
	97	6269392	2001-07-31	Cotichini, Christian , et al.	
	98	6272533	2001-08-07	Hendrick, Hendrik A., et al.	709 213
	99	6272637	2001-08-07	Little, Wendell L., et al.	713 194
	100	6282651	2001-08-28	Ashe, Vincent	
	101	6282657	2001-08-28	Kaplan, Michael M., et al.	]
	102	6292874	2001-09-18	Barnett, Philip C.	711 153
	103	6301646	2001-10-09	Hostetter, Matthew J.	
	104	6308270	2001-10-23	Guthery, Scott B., et al.	
	105	6314409	2001-11-06	Schneck, Paul B., et al.	
	106	6321314	2001-11-20	Van Dyke, Korbin S.	
	107	6339815	2002-01-15	Feng, Eugene	
	108	6339816	2002-01-12	Bausch, Jean	
	109	6357004	2002-03-12	Davis, Derek L.	
	110	6374286	2002-04-16	Gee, John K., et al.	
	111	6374317	2002-04-16	Ajanovic, Jasmin , et al.	710 105
	112	6378072	2002-04-23	Collins, Thomas , et al.	
	113	6389537	2002-05-14	Davis, Derek L., et al.	
	114	6397242	2002-05-28	Devine, Scott W., et al.	]
	115	6412035	2002-06-25	Webber, Victor	]
	116	6421702	2002-07-16	Gulick, Dale E.	]
	117	6435416	2002-08-20	Slassi, Tarik	
					]

1.1 2	to the contract of the contrac			
	118	6445797	2002-09-03	McGough, Paul , et al.
	119	6463535	2002-10-08	Drews, Paul C., et al.
	120	6499123	2002-12-24	McFarlane, Harold L., et al.
	121	6505279	2003-01-07	Phillips, Gary , et al.
	122	6507904	2003-01-14	Ellison, Carl M., et al.
	123	6535988	2003-03-18	Poisner, David L.
	124	6557104	2003-04-29	Vu, Son T., et al.
	125	6633963	2003-10-14	Ellison, Carl M., et al.
	126	6633981	2003-10-14	Davis, Derek L.

#### Remarks

Note: Remarks are not for responding to an office action.

Applicants, in accordance with their duty of disclosure under 37 CFR 1.56 and in accordance with 37 CFR 1.97(c)(2), hereby submit this Electronic Information Disclosure Statement citing U.S. Patent documents for consideration by the Examiner. Pursuant to 37 CFR 1.97, the submission of this Electronic Information Disclosure Statement is not to be construed as a representation that a search has been made and is not to be construed as an admission that the information cited in this statement is material to patentability. This Electronic Information Disclosure Statement is being filed after the mailing of a first office action and before the receipt of a final office action, notice of allowance, or an action otherwise closing prosecution. Pursuant to 37 CFR 1.97(c)(2), the fee set forth in 37 CFR 1.17(p) of \$180.00 is due for the filing of this Electronic Information Disclosure Statement. Please charge this fee and any other fee that may be due to Deposit Account 02-2666. Applicants respectfully request that the cited documents be considered and that the form be initialed by the Examiner to indicate such consideration and a copy thereof be returned to Applicants' attorney of record.

# Signature

Examiner Name	Date